February 2000
EPA Unplugged

EPA Case Study
Lessons Learned

December 11, 2002

GAO Audit Timeline

- October 1999 – GAO Audit begins
- December 1999 – GAO notifies EPA of certain vulnerabilities
- February 2000 – GAO exit interview citing serious vulnerabilities
- Due to publicity of the audit, EPA Administrator decided to disconnect Agency from Internet

Audit Findings

- Ineffective perimeter defenses
- Inadequate system access controls
- Weak network and operating system controls
- Weak security planning and risk assessment practices

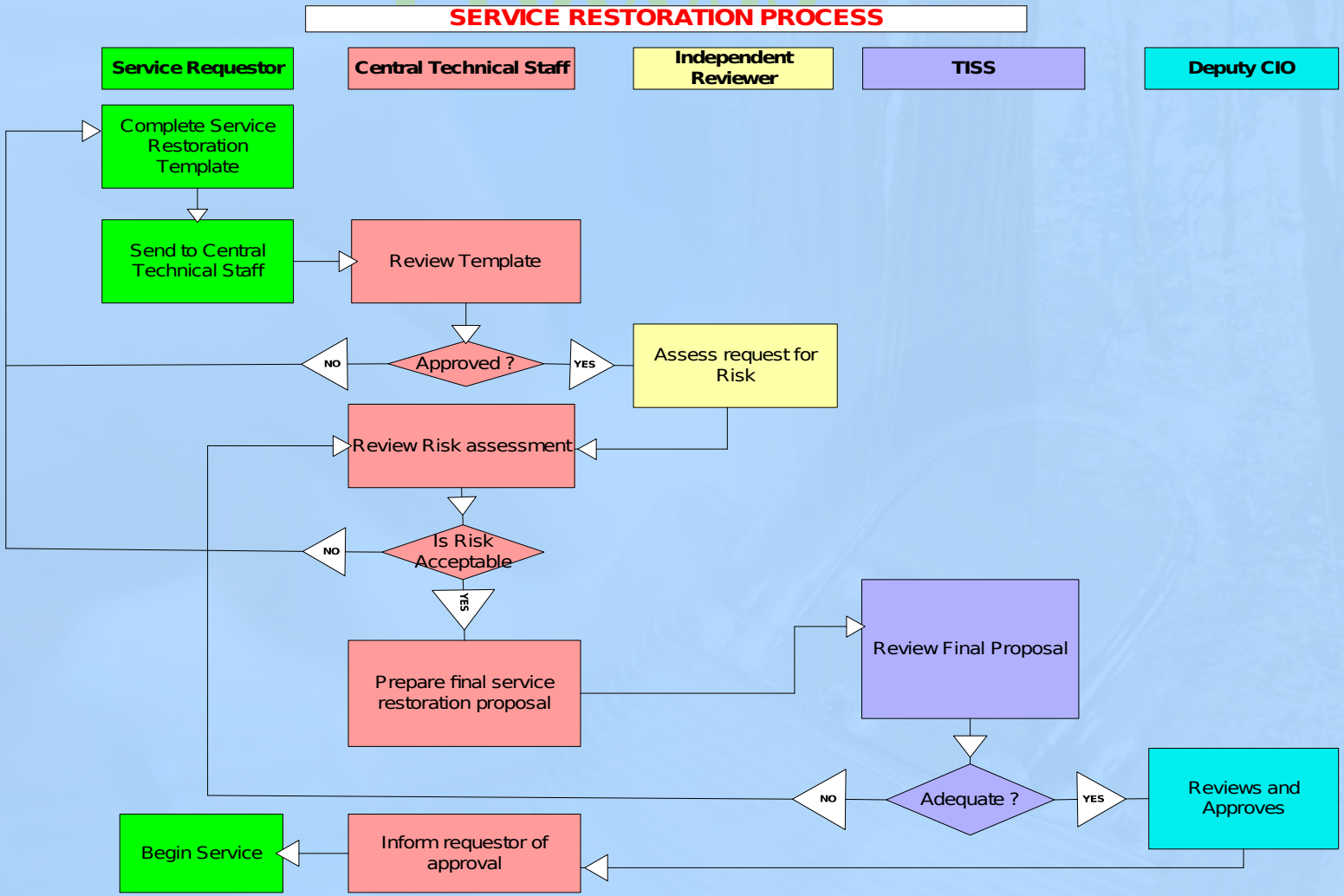
EPA Response

- Established criteria for service restoration
- Asked **Executive Management** to identify highest priority systems and services
- Worked only on **highest priorities**
- Embraced **risk based** decision making
- Improved management processes

Service Restoration Process

- Reflected new approach – deny all except where allowed.
- Risk Based
- Senior Management priorities
- Focused on:
  - Services critical to mission operations
  - Services easiest to restore
  - Services serving the widest community

Service Restoration Process



Services Restored

- 90% of services restored within 6 months including:
  - Public access to web server
  - Financial systems
  - Internet access and email for employees
- Of balance, some services never restored due to unacceptable risks

Lessons Learned

- Engage Executive Management in decision making
- Set priorities based on executive management needs
- Make risk based decisions
  - Reduce unnecessary open connections
  - Assure risks are known
  - Ensure appropriate controls in place before going live

Lessons Learned

- Better understanding of what connections are needed to do business
- Value of independent expertise
- Need for documentation
- Value of explicit decision making
- Communicate with managers and users

Conclusion

Security is the management

of risks.

Questions ?

Marian Cody, Associate Director

Technical Information Security Staff

U.S. EPA